Жук Ілона Василівна,
старший науковий співробітник наукової лабораторії з проблем протидії злочинності ННІ № 1 Національної академії внутрішніх справ, кандидат юридичних наук, доцент

АКТУАЛЬНІ ПИТАННЯ КІБЕРЗАХИСТУ ПЛАТІЖНИХ СИСТЕМ В УМОВАХ ВОЄННОГО СТАНУ: КРИМІНАЛЬНО-ПРАВОВИЙ АСПЕКТ

В умовах військового вторгнення Російської Федерації в Україну набувають особливої актуальності питання забезпечення кібербезпеки, насамперед, напрямки посилення обороноздатності держави у кіберпросторі та боротьби з кіберзлочинністю. Стратегією кібербезпеки України, затвердженої рішенням Ради національної безпеки і оборони України та введеної в дію Указом Президента України від 26 серпня 2021 року № 447 до основних загроз кібербезпеці віднесена кіберзлочинність, що «завдає шкоди інформаційним ресурсам, суспільним процесам, особисто громадянам, знижує довіру суспільства до інформаційних технологій та призводить до значних матеріальних втрат» (п. 3). Для посилення спроможності у протидії кіберзлочинності планується: завершення імплементації в законодавство України положень Конвенції про кіберзлочинність; розроблення підходів щодо реалізації державної політики у сфері забезпечення прав громадян у кіберпросторі; врегулювання на законодавчому рівні правового статусу криптовалют; запровадження практики проведення інформаційної кампанії щодо дій громадян у випадку, коли вони стикаються із кібершахрайством та іншими кіберзлочинами, тощо.

Відповідно до Закону України «Про основні засади забезпечення кібербезпеки України» від 5 жовтня 2017 року № 2163 підприємства, установи та організації, які провадять діяльність та надають послуги у банківському та фінансовому секторах віднесені до об'єктів критичної інфраструктури (ст. 6), тобто, є об'єктами кіберзахисту. Порядок, вимоги та заходи із забезпечення кіберзахисту та інформаційної безпеки у банківській системі України та для суб'єктів переказу коштів визначає Національний банк України (ст. 8). З цією метою Національним банком було розроблено Положення про захист інформації та кіберзахист у платіжних системах, затверджене Постановою Правління від 19 травня 2021 року № 43. Згідно з цим положенням суб'єкт інформаційного захисту зобов'язаний вживати заходів для забезпечення захисту інформації, кіберзахисту та інформаційної безпеки на всіх стадіях циклу системи захисту, що використовується для переказу коштів (п. 15), а у разі виявлення подій, що містять ознаки злочинів, передбачених у

розділі XVI «Кримінальні правопорушення у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку» Кримінального кодексу (далі – КК) України зобов'язаний невідкладно повідомити Національний банк. Враховуючи, що останнім часом в Україні кіберзлочинність мала тенденцію до зростання, завдаючи значної матеріальної шкоди державним інформаційним ресурсам, об'єктам критичної інфраструктури та громадянам, підриваючи довіру суспільства до безпечності використання інформаційних технологій і цифрових послуг, а у період збройної агресії Російської Федерації такі прояви ще збільшилися, Верховною Радою було прийнято Закон України «Про внесення змін до Кримінального кодексу України щодо підвищення ефективності боротьби з кіберзлочинністю в умовах дії воєнного стану» від 24 березня 2022 року № 2149. Цим законом було внесено зміни до згаданого вище розділу XVI КК, зокрема, статей 361 та 361-1. Найбільшу цікавість для нас становлять зміни, які торкнулися ст. 361 КК. Як зазначено у Пояснювальній записці до законопроекту, однією з цілей його розробки було приведення термінології КК у відповідність з вимогами законодавства України у сфері кібербезпеки і насамперед, із Законом України «Про електронні комунікації» від 16 грудня 2020 року № 1089.

Отже, ст. 361 КК «Несанкціоноване втручання в роботу інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж» отримала нову редакцію, згідно з якою було розмежовано ступінь відповідальності за передбачені діяння в залежності від їх наслідків. Стаття у чинній редакції має шість частин (тоді як попередня складалася з двох), п'ять з яких містять заборонювальні норми, та примітку. У ч. 6 закріплене роз'яснення, за яких умов визначені законодавцем дії не тягнуть відповідальності за ст. 361 КК («якщо вони були вчинені відповідно до порядку пошуку та виявлення потенційних вразливостей таких систем чи мереж»). Разом з тим, більш доцільним видається варіант розміщення такого роз'яснення у примітці до статті. Однією з найсуттєвіших змін, визначених цією статтею, є закріплення зниженого порогу відповідальності. Так, якщо за попередньої редакції це правопорушення мало матеріальний склад з обов'язковими наслідками у вигляді «витоку, втрати, підробки, блокування інформації, спотворення процесу обробки інформації або порушення встановленого порядку її маршрутизації», то наразі кримінальна відповідальність настає вже за факт несанкціонованого втручання в роботу інформаційних (автоматизованих), електронних комунікаційних,

інформаційно-комунікаційних систем та електронних комунікаційних мереж. Така зміна конструкції складу правопорушення може викликати запитання з позиції оцінки рівня його суспільної небезпечності. Як випливає із ч. 2 ст. 11 КК те чи інше діяння може бути визнане кримінальним правопорушенням лише у разі, якщо воно заподіяло чи могло заподіяти істотну шкоду фізичній чи юридичній особі, суспільству або державі. Отже, чи достатнім є рівень суспільної небезпечності, приміром, несанкціонованого увімкнення непрацюючого комп'ютера, яке не потягло за собою жодного наслідку? Вочевидь, ці питання потребують свого подальшого ретельного вивчення. Тим не менш, заслуговують на позитивну оцінку спроби удосконалення правового механізму забезпечення інформаційної безпеки в Україні, зокрема, у сфері переказу коштів.

Задніченко Сергій Іванович,
заступник начальника Департаменту документального забезпечення – начальник управління організаційного забезпечення та контролю Національної поліції України

КРИМІНАЛЬНА ВІДПОВІДАЛЬНІСТЬ ЗА РОЗГОЛОШЕННЯ ДЕРЖАВНОЇ ТАЄМНИЦІ В ПЕРІОД ВОЄННОГО СТАНУ

Указом Президента України «Про введення воєнного стану в Україні» від 24 лютого 2022 року №64/2022 було не лише введено воєнний стан, а й тимчасово (на період дії правового режиму воєнного стану) передбачено можливість обмеження конституційних прав і свобод людини і громадянина. Серед конституційних прав були й права, гарантовані ст. 34 Основного Закону України, а саме: вільно збирати, зберігати, використовувати і поширювати інформацію усно, письмово або в інший спосіб. Оскільки нині йдеться про інтереси національної безпеки, територіальної цілісності та громадського порядку, закономірним є обмеження само цих прав. Ефективна система охорони державної таємниці є однією з гарантій збереження цілісності та недоторканості будь-якої держави, незалежно від її місцезнаходження на географічній мапі світу та етапу економічного розвитку. Зокрема, в Конституції України забезпечення інформаційної безпеки розміщено серед найважливіших функцій держави (стаття 17 Конституції України). Безперечно, витік інформації, що становить державну таємницю, може спричинити підрив основних засад оборони держави, захисту державного суверенітету, конституційного ладу, територіальної цілісності України, а також дезорганізувати діяльність Збройних Сил України та інших військових формувань, функціонування надважливих